

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*INFORMATION ASSOCIATED WITH dayne@pgbmt.com
AND dayne@turbosourcetx.com, THAT IS STORED AT
PREMISES CONTROLLED BY MICROSOFT
CORPORATION, ONE MICROSOFT WAY, REDMOND, WA

Case No.

2:21-mj-754

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See attachment A.

located in the WESTERN District of WASHINGTON, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1001	False Statements
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 287	False Claims
18 U.S.C. § 38	Fraud Involving Aircraft Parts

The application is based on these facts:

See attached affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Delia McMullen, Special Agent

Printed name and title

Sworn to before me and signed in my presence. Via FaceTime

Date: November 24, 2021City and state: Newark, Ohio

 Elizabeth A. Preston Deavers
 United States Magistrate Judge


**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

**IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
dayne@pgbmt.com AND
dayne@turbosourcetx.com, THAT IS
STORED AT PREMISES CONTROLLED
BY MICROSOFT CORPORATION, One
Microsoft Way, Redmond, WA 98052**

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Delia McMullen, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Microsoft Corporation. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Defense Criminal Investigative Service (DCIS), which is part of the Office of the Inspector General for the U.S. Department of Defense (DoD). I have been so employed for approximately 19 years. In my current capacity, I am charged with investigating acts of suspected DoD contract fraud.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, to wit: Section 1001 (making false statements); Section 1343 (wire fraud); Section 287 (making a false or fraudulent claim against the U.S); and Section 38 (fraud involving aircraft parts) have been committed by **Gregory Gotreaux, WM Industries LLC dba Turbo Source**, Philip Huddleston and other unknown persons and companies. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Contracting Process

6. The United States Department of Defense (DoD) contracts through its various agencies, such as the Defense Logistics Agency (DLA). DLA is the United States’ combat logistics support agency, and as such manages the global supply chain for all military services, 10 combatant commands, other federal agencies, and partner and allied nations. DLA has three primary depots that manage the military’s global supply chain – DLA Land and Maritime (L&M)

in Columbus, Ohio; DLA Aviation in Richmond, Virginia; and DLA Troop Support (TS) in Philadelphia, Pennsylvania.

7. When the DoD determines that a particular part is needed, the DoD issues “Solicitations,” or Requests for Quotation (RFQs) electronically through a web-based application, DIBBS (DLA’s Internet Bid Board System). Users (potential contractors) are able to search for, view, and submit secure quotes based upon the RFQs for the items DLA is looking to obtain. The solicitations (RFQs) list the DoD requirements, which can include drawings and/or specifications, such that any potential contractor is aware of exactly how the part is to be made or where they can obtain the part. DoD contractors are required to have a quality control system in place to ensure the parts supplied to the DoD are in accordance with DoD drawings and specifications. In addition to noting the contractor’s agreement or disagreement with the requirements of the solicitation, the quote, or bid, submitted will list the contractor name, business location, and an email address.

8. To conduct business with the DoD, contractors must register in the System for Award Management (SAM), to include providing an email address, and agree to receive payments electronically. The contractors must also obtain a Commercial and Government Entity (CAGE) code. The CAGE code is a 5-character identification number used extensively within the federal government, assigned by the DLA. The CAGE code is used to support a variety of mechanized systems throughout the government and provides a standardized method of identifying a given contractor facility at a specific location.

9. In the contracting process, once parts are shipped to the DLA, contractors enter the shipping and invoicing information electronically, through a secure, web-based system, which allows the government to receive and pay electronically. Upon receiving the invoice, the DoD, through the Defense Finance and Accounting Service (DFAS), Columbus, Ohio; in the Southern

District of Ohio, will issue electronic payment to the supplying contractor and retain a voucher as a record of the payment.

10. DLA L&M in Columbus is also home to laboratories used to test and identify nonconforming parts sold to DLA, including the capability to test for counterfeit material, substitute inferior products, nonconforming parts, and remark/over brand items. These laboratories at DLA L&M are used to test all suspect parts provided to DLA worldwide.

Turbo Source

11. On November 25, 2018, **Turbo Source** was registered in the SAM by **Gregory Gotreaux**, and received its CAGE Code of 87PR5 on December 24, 2018. On March 26, 2021 **Gotreaux** submitted **Turbo Source's** most recent updated information to the SAM, which is required to be done once per year. In both **Turbo Source's** original registration and annual update to the SAM, **Gotreaux** listed a physical address for **Turbo Source** of 5770 Kohler Street, Beaumont, TX 77706. **Gotreaux** also identified himself in the SAM as the owner/president of **Turbo Source** as well as the individual who entered the information in the SAM – called the “Individual Executing Consent”. The email addresses that **Gotreaux** entered for the company in the SAM entries were dayne@pgbmt.com and dayne@turbosourcetx.com.

12. According to **Turbo Source's** contract history with the DoD, the company began bidding on and receiving DLA contracts in November 2019. Since then, **Turbo Source** has received approximately \$774,977 obligated DLA contracts.

13. A query in the CLEAR database of **Gregory Gotreaux's** social security number revealed that he owns a business called **WM Industries LLC dba Turbo Source**. Per the report, the business was started in 2020, is owned by **Gregory Gotreaux** and Philip Huddleston, and is located at 5770 Kohler Street, Beaumont, TX 77706. According to this same CLEAR report, this

address is also the residence of **Gotreaux**. A review of this address on Zillow revealed a one-story single family house, 1,378 square feet in size. The exterior of the house appears to be composed of brick and yellow siding.

14. On September 6, 2021, a search of the Jefferson County, TX Central Appraiser District website and confirmed that **Gotreaux** is the current owner of 5770 Kohler Street, Beaumont, TX 77706.

15. As part of its ongoing quality assurance efforts, during June 2020 through January 2021 DLA L&M requested via email that **Turbo Source** provide traceability documentation on ten of these contracts, cumulatively valued at \$219,781.40. **Turbo Source** was paid, via electronic wire transfers, for all of these parts by DFAS in Columbus, OH. These parts consisted of primarily mechanical parts, such as engine oil pump assemblies, piston connecting rods, turbo superchargers, etc., used in various U.S. Army, Navy and Air Force weapon systems. Some of the parts are critical application items. All of the parts for these ten contracts were required to be manufactured by the approved sources of either Caterpillar Inc. or MTU America Inc., and **Gotreaux** certified in his bids to DLA for all ten contracts that he would provide the exact authentic parts from the specific approved source (which depending on the contract was Caterpillar or MTU America). **Gotreaux** responded to all ten requests for trace documentation from DLA L&M using the email accounts of dayne@pgbmt.com and dayne@turbosourcetx.com. In his email responses to DLA, **Gotreaux** attached quotes and invoices from authorized Caterpillar or MTU America dealers and claimed to have purchased the authentic parts from these dealers. These dealers consisted of Rush Truck (four contracts), Stewart and Stevenson (four contracts) and PC Industries (two contracts).

16. During late 2020 through early 2021, a DLA L&M Quality Assurance Specialist (QAS) contacted all three dealers, and provided them the invoices and quotes that **Gotreaux** had

emailed to DLA L&M. The dealers told the QAS that nine of the ten sets of invoices and quotes were falsified and that **Gotreaux** had not purchased the parts from them. Regarding the remaining invoice and quote, per the dealer, PC Industries, the quote and invoice were authentic but were for remanufactured turbo superchargers, not new, originally manufactured turbo superchargers (which **Gotreaux** had certified he would provide in his bid to DLA for the contract). Per PC Industries, their price at the time for the remanufactured turbo superchargers was \$1,850 and for the new turbo superchargers was \$4,779.

17. Based upon this information, DCIS opened a criminal investigation into **Turbo Source** and **Gotreaux** in January 2021.

18. The above ten contracts, which were issued by DLA L&M to **Turbo Source** between January 2020 and December 2020, were “code and part” contracts. Contracts issued by DLA are typically one of two types of contracts: “drawing” contracts or code and part contracts. On a drawing contract, the contractor is required to manufacture a specific part in accordance with specifications identified by DLA in its solicitation and contract. On a code and part contract, the contractor is required to provide DLA a specific part that was manufactured by a specific approved source(s); DLA identifies the specific part and approved source(s) in its solicitation and contract. Further, the contractor certifies in its bid, for the code and part contract, that it will provide the required specific part from the required specific source. **Turbo Source** was required to provide DLA specific parts manufactured by specific approved sources, but instead sold nonconforming parts from unapproved sources.

19. For example, **Turbo Source** obtained DLA contract SPE7L5-20-P-0607 on March 3, 2020 and subsequently provided 18 diesel engine cylinder heads to DLA at a price to DLA of \$61,200. These parts are critical application items used on or in support of the F-18 Growler fighter

jet. Per the contract, the diesel engine cylinder heads were required to be part number 5102770, manufactured by MTU America. **Gotreaux** certified in his quote for this contract, which he submitted online in DIBBS on December 12, 2019, that **Turbo Source** would provide part number 5102770 from Cage Code 72582 (this is MTU America's cage code). When requested by a DLA L&M Contracting Officer to provide trace documentation to verify that **Turbo Source** had supplied the correct parts to DLA, on August 25, 2020, **Gotreaux** emailed the Contracting Officer a falsified invoice reflecting that he had purchased 18 MTU America cylinder heads, part number 5102770. The email address that **Gotreaux** used to send this email was dayne@turbosourcetx.com.

20. Each one of **Turbo Source's** quotes for the above ten contracts contained the following "Quoter" information:

Name: Gregory D Gotreaux
Phone: (409) 554-5507
Email: dayne@pgbmt.com

21. Each one of **Turbo Source's** quotes for the above ten contracts also contained the following "Vendor Address" information:

Gotreaux, Gregory D DBA Premier
5770 Kohler St.
Beaumont, TX 77706-6327
US

22. A review of DFAS records for the ten referenced contracts revealed **Turbo Source** electronically invoiced DFAS for payment of these contracts and that DFAS electronically paid **Turbo Source** a total of \$219,781.40 for the ten contracts based upon the invoices **Turbo Source** submitted.

23. On September 23, 2021, DLA issued a Notice of Proposed Debarment on **Turbo Source, Gotreaux** and Philip Huddleston.

24. On October 27, 2021, **Gregory Gotreaux** was interviewed and stated **Turbo Source** was Philip Huddleston's idea, he was a partner in **Turbo Source**, and had invested money in the business with the intent of splitting profits of the business once his investment had been repaid. **Gregory Gotreaux** admitted to purchasing cheaper unapproved parts and creating false invoices he sent via email to DLA in response to DLA's traceability requests and Philip Huddleston had knowledge of this and evidence of such would be contained in the emails they sent each other. **Gregory Gotreaux** knew this was wrong but indicated Philip Huddleston said they would not get caught and the government would not find out or look at the vendors they were using.

25. On November 9, 2021, a preservation letter was served on Microsoft Corporation. Microsoft Corporation responded on November 16, 2021, and provided the preservation record number: **GCC-1785515-C8T3X9**. In general, an email that is sent to a Microsoft Corporation subscriber is stored in the subscriber's "mail box" on Microsoft Corporation's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft Corporation's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft Corporation's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

26. In my training and experience, I have learned that Microsoft Corporation's provides a variety of on-line services, including electronic mail ("email") access, to the public. Microsoft Corporation's allows subscribers to obtain email accounts at the domain name yahoo.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with

Microsoft Corporation. During the registration process, Microsoft Corporation asks subscribers to provide basic personal information. Therefore, the computers of Microsoft Corporation are likely to contain stored electronic communications (including retrieved and unretrieved email for Microsoft Corporation subscribers) and information concerning subscribers and their use of Microsoft Corporation services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. An Microsoft Corporation subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft Corporation. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

28. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

29. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

30. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

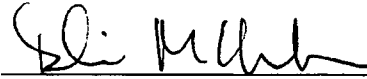
31. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

32. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft Corporation, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Delia McMullen
Special Agent
Defense Criminal Investigative Service

Subscribed and sworn to before me on November 24, 2021


Elizabeth A. Brown, District
United States Magistrate Judge

JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email accounts dayne@pgbmt.com and dayne@turbosourcetx.com that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, One Microsoft Way, Redmond, WA 98052.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 9, 2021 and assigned preservation record number: **GCC-1785515-C8T3X9**, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from December 24, 2018 through the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 1001 (making false statements), Section 1343 (wire fraud), Section 287 (making a false or fraudulent claim against the U.S), and Section 38 (fraud involving aircraft parts), those violations involving **Gregory Gotreaux, WM Industries LLC dba Turbo Source**, Philip Huddleston and other known and unknown persons and companies, and occurring on or after December 24, 2018, including:

- Information related to U.S. Department of Defense (DoD) contracting, to include but not limited to, solicitations, bids/quotes, purchase orders/contracts, DFAS or other payment records, inspection records or results including any drawings or certifications whether conducted in-house or by a government agency such as DCMA or a private third-party; traceability documents or requests for traceability; the ordering or manufacturing of any parts provided to the DoD including any receipts, invoices, correspondence with suppliers; the shipping of parts from suppliers and to the DoD.
- Information related to the creation, ownership, registration, corporate meeting minutes, tax records and annual reports, employees or dissolution of **WM Industries LLC dba Turbo Source**; the extent of their dealings with the DoD and any of its agencies to include any records of CAGE code or SAM applications or registrations, pre-award survey documents, quality manuals and correspondence with DoD;
- Records and information relating to fraud committed against the DoD and any of its agencies;
- Records and information relating to the use of e-mail accounts;

- Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Microsoft Corporation, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Microsoft Corporation. The attached records consist of _____.
[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Microsoft Corporation, and they were made by Microsoft Corporation, as a regular practice; and

b. such records were generated by Microsoft Corporation's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Microsoft Corporation in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Microsoft Corporation and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature